Claims 1, 12 and 21 are amended.

Claims 1, 4-12, 16-21 and 24-28 remain in the application and are listed as follows:

**1.     (Currently Amended)**     A method, comprising:

receiving data input through a web page from a client device;

referencing a declarative module to determine a client input security screen to apply to the data input from the client device, wherein the declarative module comprises:

a global section that includes at least one client input security screen that applies to any type of client input value; and

an individual values section that includes at least one client input security screen that applies to a particular type of client input value; and

applying multiple client input security screens to the data input from the client device, including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module, wherein the client input security screens are distinct from one another, and wherein one or more predetermined symbols are removed without replacement from the data input, and wherein said act of referencing comprises first using the global section to screen one or more client input values and then using the individual values section to screen at least one of said one or more client input values.

**2.     (Canceled)**

2

**3.** **(Canceled)**

**4.** **(Previously Presented)** The method as recited in claim 1, wherein the particular type of client input value is one of the following types of client input values: query string; server variable; form value; cookie.

**5.** **(Previously Presented)** The method as recited in claim 1, wherein the declarative module further comprises a web.config file.

**6.** **(Original)** The method as recited in claim 1, wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen.

**7.** **(Original)** The method as recited in claim 1, wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen.

**8.** **(Original)** The method as recited in claim 1, wherein a client input security screen further comprises one or more values that may be entered as client input, the one or more values further comprising the only values that may be entered as client input.

3

**9.** **(Original)**   The method as recited in claim 1, wherein a client input security screen further comprises one or more screened values that, when detected in the client input, cause an action to be taken on the client input.

**10.** **(Original)**   The method as recited in claim 9, wherein the action to be taken further comprises removing the one or more screened values detected in the client input.

**11.** **(Original)**   The method as recited in claim 9, wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input.

**12.** **(Currently Amended)**   A system, comprising:

a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network;

means for receiving client input data;

a declarative module configured to include multiple client input security screens that declare screening rules for client input, wherein the declarative module comprises:

a global section that includes one or more client input security screens that are applied to all types of client input; and

an individual values section that includes one or more client input security screens that are applied to specified types of client input; and

a client input security screening unit configured to apply the screening rules for client input to the client input data and to perform one or more actions on

4

invalid client input data, wherein the screening rules are from distinct client input security screens from the global section and the individual values section, ~~and wherein the client input security screening unit is further configured to remove without replacement one or more predetermined symbols from the client input data,~~ and wherein the client input security screening unit is configured to first use the global section to screen one or more client input values and then use the individual values section to screen at least one of said one or more client input values.

**13.** **(Canceled)**

**14.** **(Canceled)**

**15.** **(Canceled)**

**16.** **(Original)** The system as recited in claim 12, wherein a screening rule further comprises a client input variable that may be accepted as input from a client.

**17.** **(Original)** The system as recited in claim 12, wherein a screening rule further comprises one or more screened characters that, when detected in client input, are screened from the client input according to a screening rule.

5

**18.**	**(Original)**	The system as recited in claim 17, wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action.

**19.**	**(Original)**	The system as recited in claim 17, wherein the screening rule further comprises a specified screening action that is applied to the screened client input.

**20.**	**(Previously Presented)**	The system as recited in claim 12, wherein the declarative module further comprises a web.config file.

**21.**	**(Currently Amended)**	One or more computer-readable storage media containing computer-executable instructions that, when executed on a computer, ~~perform the following steps~~ implement a method comprising:

serving a web page to a client over a distributed network;

receiving client input via the web page;

comparing the client input with multiple and distinct client input security screens stored in a security declarative module, wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values, wherein the global section is used to first screen one or more client input values and then the individual values section is used to screen at least one of the one or more client input values;

if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module; and

wherein the client input security screens included in the security declarative module can be applied to multiple web pages; and

wherein one or more predetermined symbols are removed without replacement from the client input.

**22.** **(Canceled)**

**23.** **(Canceled)**

**24.** **(Previously Presented)** The one or more computer-readable media as recited in claim 21, wherein the security declarative module further comprises a web.config file.

**25.** **(Original)** The one or more computer-readable media as recited in claim 21, wherein the screening action further comprises an action specified in a client input security screen.

**26.** **(Original)** The one or more computer-readable media as recited in claim 21, wherein the screening action further comprises a default action that is not required to be specified in a client input security screen.

**27.** **(Original)** The one or more computer-readable media as recited in claim 21, wherein the multiple web pages are included in a web project.

28. **(Original)** The one or more computer-readable media as recited in claim 21, wherein the multiple web pages are included in a web-based application.